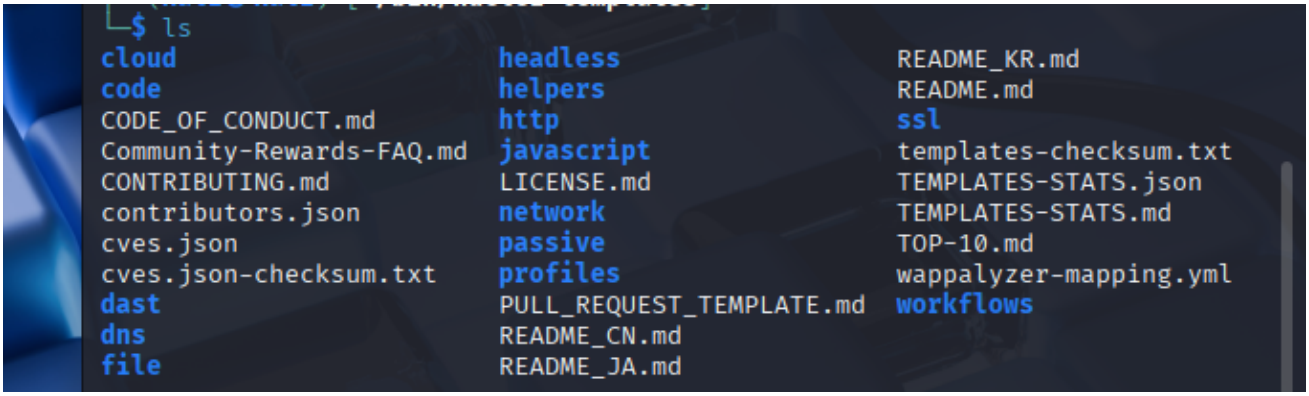
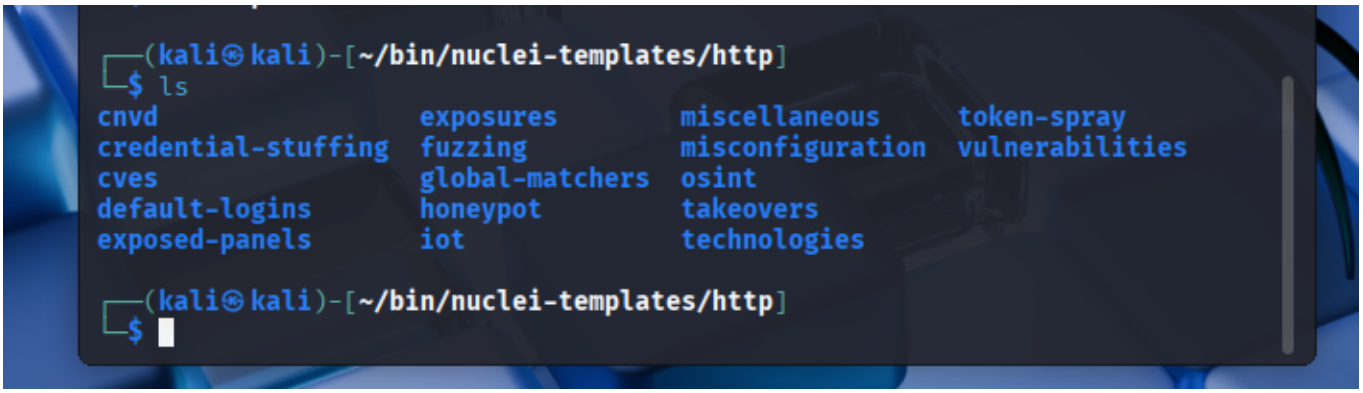
neclei scanner

- هي اداه موجود جواها templet جاهزه توصلك للثغرات
- جوهاه اكتر من 8000 templet جاهزه مكتوبه بلغه GO
- خلي بالك ان المواقع بتمنع استخدامها في الغالب
- عشان الاداه دي تاخد حقها شغلها علي vps برام 64 ويفضل اعلي
- ممكن تستعمل مواقع زي discovery project
- اعمل اميل علي www.digitalocean.com اعمل اكونت هتاخد 200 دولار منه تاخد بيهم vps لمده شهرين

- بتنزلها من github وكمان معاها templet لازم تنزلها عشان تقدر تعمل scan
- 

- دول ال هتلاقيهم جواه templet
- اهمهم لينا http



- ودا ال جواها دي الحاجات الي هيدورلك عليها زي cve

تحديد هدف واحد

nuclei -u https://target.com

تفعيل كل ال template

nuclei -u https://target.com -t / مكان تنويل ال template

فحص قائمة URLs من ملف

nuclei -l urls.txt

استخدام template أو مجلد templates

nuclei -u https://target.com -t cves/2022/CVE-XXXX.yaml
nuclei -u https://target.com -t vulnerabilities/

تحديد مستوى الخطورة

nuclei -u https://target.com -severity high,critical

حفظ النتائج في ملف

nuclei -u https://target.com -o results.txt

تحديد عدد الطلبات في الثانية

nuclei -u https://target.com -rate-limit 20

تمرير الفحص عبر بروكسي

nuclei -u https://target.com -proxy http://127.0.0.1:8080

إضافة headers مخصصة

nuclei -u https://target.com -H "Authorization: Bearer TOKEN"

طباعة النتائج بصيغة JSON

nuclei -u https://target.com -json

الوضع التفصيلي verbose

nuclei -u https://target.com -vv

تحديث التمبلتات

nuclei -update-templates

```
root@kali:~# nuclei -u https://testphp.vulnweb.com -o file.txt -mhe
 4
```

- **-mhe**
  - دا بيكون لو عاوز الاداه تبعت لكل موقع عدد معين من الطلبات
    لان الاداه بتبعت 30 طلب

```
^C[INF] CTRL+C pressed: Exiting
[INF] Attempting graceful shutdown...
[INF] Creating resume file: /root/.cache/nuclei/resume-cr3737uen10vgv
orqeh0.cfg
root@kali:~#
root@kali:~# nuclei -resme
```

- ممكن تستخدم الامر resme لو وقفت الاداه هو بيعملك ملف بالاسم دا اتسخدم الامر ب عشان تكمل scan في وقت تاني

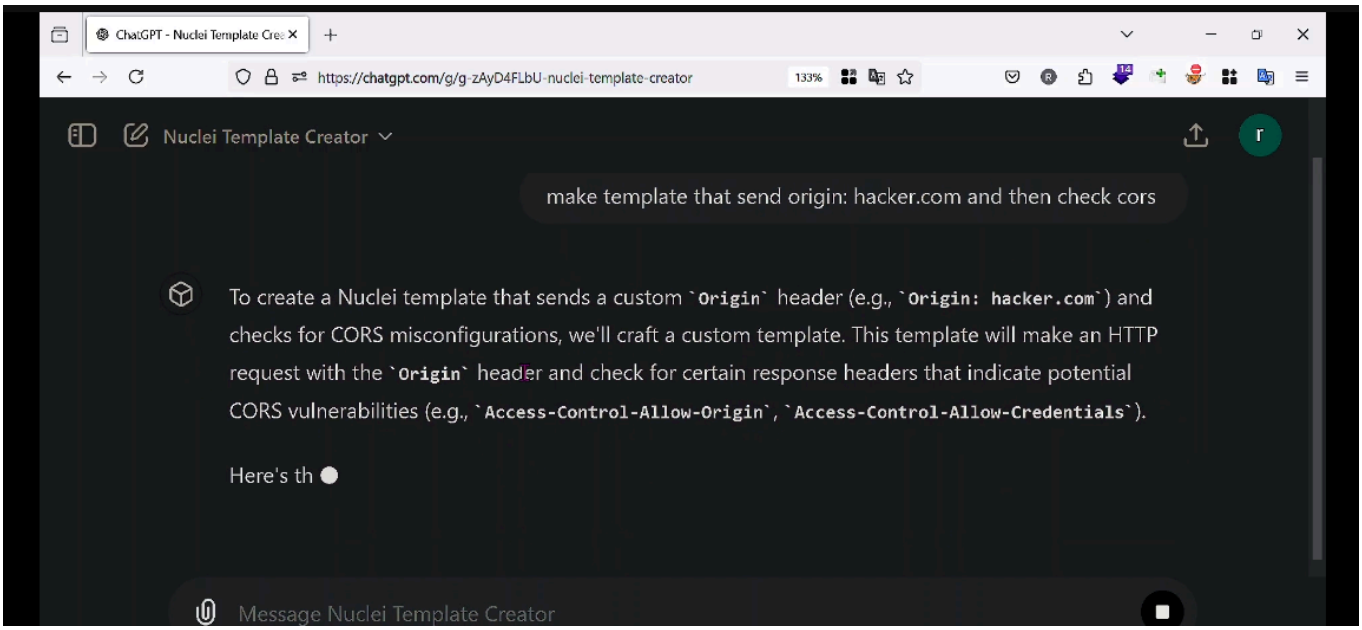
```
        -> nuclei -u https://api.swisscom.com


=> rate limit => rate limit headers
                - X-Forwarded-For: 127.0.0.1
                - X-Forwarded-Host: 127.0.0.1
                - X-Forwarded: 127.0.0.1
                - Forwarded: 127.0.0.1
```

- ممكن تستعمل اجزاء rate limit عشان ما تاخدش block عن طريق -H

- لوعاوز تعمل templet خاصه بيك
- اول حاجه نت بتقوله نت عاوز يكون اي في الطلب ونت متوقع اي في في الرد
- وعلي الاساس دا بتقيس الثغره زي cors مثلا بتحط orign:hacker.com ومستني الرد يكون في

- access-control-allow-origin



- في module كامل في chatgpt يساعدك انك تعمل كدا بكل بسهوله

```
Accept: "../../../../../../../etc/passwd{i"
```

- payload دا ممكن يعملك RCE

- عشان تحفظ ال templet بتعمل nano file.yaml
- وتحفظ فيه كل templet ال نت عملتها
- وبعدين تقدر تستعمله عادي مع الاده عن طريق t-

-